IDS 493 Reflection Essay

Eric M. Preston

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

April 25, 2025

Abstract

This reflection paper focuses on three specific skills I've gained from my interdisciplinary cybersecurity courses during my time at Old Dominion University. The most prominent skills that have highlighted my growth in these three years are Research, Programming, and Critical Thinking. These skills have been gained through multiple research papers, programming assignments, case analyses, and group projects that have forced me to learn how to adapt and improve on what I've done before. Careful analysis of these artifacts will reveal how each has played a significant role in my academic development and readiness for a career. My ability to adapt to the multiple changes throughout my academic career has been supported by the application of interdisciplinary research and projects.

Keywords: Cybersecurity, research, programming, critical thinking, development

Introduction

In these three years at ODU, I've dealt with increasingly difficult academic challenges that have forced me to change my approach multiple times within the Cybersecurity Program. This doesn't just include my methodology for working, but it also includes my perception of cybersecurity, its changing purpose within different fields, the breadth of utility it can have, and the harms it can cause. This has also resulted in the collection of labs, research papers, coding assignments, presentations, networking maps, and more to tangibly represent that change. But, in working through each of these projects, they have been instrumental in developing what I consider to be my key skills to represent my capabilities within the cybersecurity workforce for the future. The three primary skills that I have developed from my interdisciplinary courses include research, programming, and critical thinking. To properly highlight these, it has required me to reflect and gain further insight into the value of these artifacts and how they have helped me improve.

Skill 1 - Research

Due to cybersecurity still being a relatively new field of study, the capability to research topics to lead to new conclusions is a significant skill for pushing the field forward. This not only allows for fruitful research in multiple domains that may have seemingly nothing to do with cybersecurity, but also generates professionals who can apply a research-focused approach to discussions, as well as a more analytical approach to developing solutions for cybersecurity issues. The artifacts I have chosen for this section represent my ability to tackle different topics within the field of cybersecurity and come to a new conclusion.

Artifact 1 - CYSE 200T: SCADA Systems Write-Up Assignment

This was one of the first classes that I had taken on cybersecurity during my time at ODU, and it helped to build the foundation for what I know and how I approach cybersecurity. This artifact in particular was one of the first research assignments I worked on, and its focus was on Supervisory Control and Data Acquisition (SCADA) systems, which are systems that control critical infrastructure. The fundamental problem, however, with these systems is that security isn't considered when they are being developed, leaving them more susceptible to cybersecurity attacks. During that time, the paper was fine in its requirements, but it still felt difficult at the time due to my lack of experience with researching cybersecurity topics. But, with enough time and research on how to address each desired topic, I was able to finish the paper with little difficulty. Looking back on the paper, it feels very simple in comparison to something that I could do now if I wanted to go back to the topic, showing how much I've developed my skills when it comes to researching.

Artifact 2 - CS 462: Blog Term Paper

CS 462 as a class was initially difficult for me for a different reason compared to its chosen artifact. The initial challenge of the class was being introduced to computer science, a field that I had never tackled before, which tested my ability to adapt to different information in a challenging way. However, by the end, I was given the mindset needed to approach the final project for the class, that being a paper on analyzing a recent cybersecurity breach. But this paper wasn't like previous assignments on data breaches, where the purpose was to answer only one question about it; the focus was to create a timeline of events, analyze them, break down the reasons as to why the breach occurred, and understand the greater impact that resulted from it. All of this, combined with the emphasis on technological capabilities, led to a challenging but fair paper that highlighted the critical need for cybersecurity to be implemented within the medical industry (Office for Civil Rights (OCR), 2024). I also saw it as a smaller example of the kinds of projects that would appear in later semesters.

Artifact 3 - CYSE 526: Final Research Paper Project

In CYSE 526, the course focused on cyber warfare and the implications of cybersecurity at the national and international scale. The final project for the course was a research paper that involved cyber war and was a topic of your own choice. Due to the rise in Artificial Intelligence (AI) in the past few years, I felt it was a topic that was worth writing about, both to see how the topic from a security perspective is handled at different levels and to better understand it as a concept to know whether or not it is as dangerous as commonly perceived (Tyson & Kikuchi, 2023). While this seems fine on paper, the artifact itself was extremely large in needed content, requiring me to implement the entire history of AI as a prelude to how it's implemented at multiple levels, showing multiple aspects of issues, and changing perspectives based on the scale I was at utilizing a literature review and methodology. It has remained by far the most researched cybersecurity-related topic I have ever done, and while very taxing, I came out the other end much more knowledgeable on AI than I had thought I would initially. Presently, I now see it as the best test of my capability to research, understand new topics, and present new solutions.

Skill 2 - Programming

While having an understanding of cybersecurity from a research perspective is beneficial, it is also crucial to have hands-on experience with cybersecurity tools and applications to know how to defend against malicious attacks. This can include things like programming languages and operating systems, which can help in developing security controls. This next set of artifacts shows how I developed my capabilities with programming and applied them in different circumstances.

Artifact 1 - CYSE 250: Socket Programming Group Project

This class was my first introduction to the programming language Python, and the culmination of that experience was with a group project around socket programming. For an artifact like this, it required creating a “server” and a “client” that would communicate with each other for a small task. With socket programming, the primary difficulty is having to code two different programs and switching between them for the needed communication. Our group went with recommendations for restaurants based on the amount of money someone had and the location they were at. The initial mistake my partner and I made was scaling the necessary data to be extremely large, so I took initiative to scale things down to a feasible level to finish in the few weeks given for the assignment, and set up schedules for us to work on the project together. By the end of the allotted time, my partner and I had created a presentation for the project and executed our code, having it work as expected and getting a perfect score. While there was difficulty with the coding, my partner and I were able to learn off of each other, and the project was a good experience for flexibility within groups, and setting up the foundation for my interest in coding.

Artifact 2 - CYSE 301: Ethical Hacking Assignment

CYSE 301 introduced me to Kali Linux, a more security-focused version of Linux, which provides additional security tools and the same capabilities as the original operating system. An example of the effectiveness of these tools appears in this artifact around ethical hacking. While there was a guide within the assignment with clear steps, the difficulty was always present with figuring out which necessary commands were needed and ensuring that I didn’t accidentally backtrack multiple steps with one wrong one. Breaking through multiple Virtual Machines (VMs), utilizing penetration testing software, and even security tools like EternalBlue were significant challenges to work through (Fairfield-Sonn, 2017). However, I can say that by the end of this assignment, I grew to understand some of the complexities of ethical hacking and can now better work with controls like Metasploit, reverse shells, and custom payloads. Finally, while I don't see myself going into the field of ethical hacking within cybersecurity, I can utilize the mindset of an ethical hacker for a better understanding of how to break through systems and can collaborate more with professionals for hardening systems.

Artifact 3 - CS 151: Programming Assignment on Classes

One of my hardest technical classes that I've had to get through has been my introductory Java class. While I had learned about Python back in CYSE 250, learning a new programming language was still a difficult experience with a lot of bumps in the road. But, I've ended up liking it more than Python due to the difficulty it presents and its further utility in the workforce for application and software design. The artifact that I felt represented my new capabilities with the language was centered around classes. To explain, classes are essentially the blueprint for the executing parts of a program, that being objects, and classes can be utilized in multiple ways (Melton & Tempero, 2007). The reason this assignment was so important was due to the incorporation of multiple topics throughout the semester, such as methods to do specific tasks, loop statements to read through the program, and try blocks to open a downloaded file with content and catch blocks to account for errors. It was difficult not only to incorporate all of these concepts and more, but also to get everything to run correctly without any kind of errors occurring. To me, that was when the language clicked for me, and I now feel motivated to continue learning about programming with Java outside of the classroom for my future career development.

Skill 3 - Critical Thinking

Cybersecurity is a field that is not only technology-based, it also overlaps with most fields by being interdisciplinary, and that is due to the integration of technology over time. To properly defend these different fields with different situations, it requires being able to critically analyze the factors at play and develop new understandings from multiple perspectives. Furthermore, looking into specific fields such as philosophy, policy, ethics, and law can also develop knowledge of cybersecurity by combining these fields to lead to new solutions. These artifacts reflect this approach for considering multiple angles for any problem to lead to a new understanding.

Artifact 1 - PHIL 355E: Professional Ethics Case Analysis

Cybersecurity Ethics was a tough but mentally rewarding class for how I approach cybersecurity. An artifact from that class that I'm proud of focused on a case of what it means to have professional ethics, for a client, if the public can end up being hurt by them. The difficult aspect of this project was not only having to utilize the perspectives of multiple codes of ethics equally to make my position, but also to use an ethical theory to further support, but inherently restrict my position. While challenging to write, the conclusion of multiple implicit social contracts between clients, employees, and the public was something that I was only able to determine by critically assessing professional ethics and how they can be applied in different contexts. Working through a paper like this not only gave me further insight into how employees connect with multiple parties, but also that for my professional career, I need to be aware of the negative outcomes that could appear due to how I apply my profession.

Artifact 2 - CYSE 425W: Ethics of Proposed Policy Paper

This course, while largely hands-off, still provided a significant amount of challenge with the desired projects on cybersecurity policy. The requirement for this artifact was to research the ethical implications of a student-created policy. For me, I went with financial incentives for companies to invest in policy due to previous internship experience, and the common problem of companies investing in cybersecurity practices after being attacked (Mejia, 2019). The conclusion of that paper required seeing how financial incentives are not always beneficial for the security of an organization, depending on the financial incentive at play, and how they can affect significant decision-makers and the customers that are affected by breaches. In the end, I enjoyed my time with the artifact because it challenged me to think critically about financial incentives from a new perspective and come to a new conclusion that would help in the future, both for the course itself and for future analysis of organizational decisions within the cybersecurity workforce.

Artifact 3 - CRJS 406: Group Tabletop Project

This final class was an interesting experience for me, as it stepped into the field of cyber law and the difficulties that exist in integrating cybersecurity into legal fields due to cybersecurity's interdisciplinary nature. This can include topics like cyberwarfare and cyberterrorism, or the difficulty of attribution when cybersecurity is involved (Appazov, 2014). The culmination of this push and pull was a group project where my team and I had to create a hypothetical cyber-attack that was at a country-wide scale, and present how all necessary U.S. federal agencies would counteract it. For our group, work was split evenly so that everyone had a role with the project, and while I had the role of detailing the hypothetical, all of us still had to collaborate on which agencies would be involved and how in the context of the attack. Furthermore, due to my knowledge of the attack's methods, I took the initiative in directing the approach for the final presentation and offering additional information for questions that people had at the end. However, each of my group members still offered their different perspectives on the project and played a part in its final presentation. This artifact helped me understand the value of different perspectives on projects and how it can force critical thinking to be a pertinent factor in new solutions.

Conclusion

Developing my ePortfolio and working through this reflection has been fruitful in teaching me how to understand what I am capable of. My research skills have grown from each project I've done, and each artifact has been an increasing trial of difficulty, which forced me to improve my research approach to tackle the next larger project. My programming skills have developed considerably, as I now understand multiple programming languages, ethical hacking concepts, and have utilized multiple security tools over time to work within the attacking and defending sides of cybersecurity. My ability to think critically about cybersecurity has been tested with contesting against and for specific ethical perspectives, forms of policy, and the interdisciplinary integration of multiple fields to address greater potential problems. At this point, with one more year before I graduate, I look forward to the new challenges that await me and hope to continuously improve as I enter my future career.

References

Appazov, A. (2014). *Legal Aspects of Cybersecurity*. https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Fairfield-Sonn, J. (2017). *WannaCry, EternalBlue, SMB Ports, and the Future* (pp. 1–9). https://www.cs.tufts.edu/comp/116/archive/fall2017/jfairfieldsonn.pdf

Mejia, G. (2019). *Examining the Impact of Major Security Breaches on Organizational Performance: Should Investing in Cybersecurity Be a Requirement for Companies?*(Order No. 27540799). Available from ProQuest Dissertations & Theses Global. (2320957589). http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/examining-impact-major-security-breaches-on/docview/2320957589/se-2

Melton, H., & Tempero, E. (2007). An empirical study of cycles among classes in Java. *Empirical Software Engineering*, *12*(4), 389–415. https://doi.org/10.1007/s10664-006-9033-1

Office for Civil Rights (OCR). (2024, April 19). *Change Healthcare Cybersecurity Incident Frequently Asked Questions*. Www.hhs.gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

Tyson, A., & Kikuchi, E. (2023, August 28). *Growing Public Concern about the Role of Artificial Intelligence in Daily Life*. Pew Research Center. https://www.pewresearch.org/short-reads/2023/08/28/growing-public-concern-about-the-role-of-artificial-intelligence-in-daily-life/